

10/688,026

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 7 日
Date of Application:

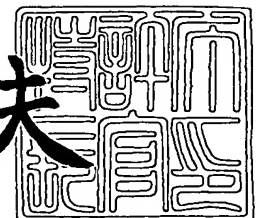
出 願 番 号 特 願 2 0 0 2 - 3 0 2 4 3 9
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 0 2 4 3 9]

出 願 人 株式会社日立製作所
Applicant(s):

2 0 0 3 年 1 0 月 1 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 8 4 5 7 6

【書類名】 特許願

【整理番号】 K02010221A

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 荒井 正人

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

 【氏名】 甲斐 賢

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

 【予納台帳番号】 013088

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書**【発明の名称】 ポリシー設定支援ツール****【特許請求の範囲】****【請求項 1】**

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、前記ポリシー情報の作成に要する作業負荷を軽減するためのポリシー設定支援ツールであって、

当該ポリシー設定支援ツールは、アクセス主体となるサブジェクトの種類毎に用意した情報と、アクセス対象となるオブジェクトの種類毎に用意した情報から、適切なポリシーを作成するものであり、

前記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、

前記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報とからなり、

更に前記ポリシー設定支援ツールは、前記サブジェクトの動作を監視して前記アクセスログ情報に記録するためのアクセス監視部と、前記サンプル情報と前記インストール情報とを照合して差分を検出する差分検出部と、前記サンプル情報と前記関連付け情報と前記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による更なるポリシーの修正および保存をするためのユーザインタフェース部とから構成されることを特徴とするポリシー設定支援ツール。

【請求項 2】

請求項 1 記載のポリシー設定支援ツールであって、

前記ポリシー設定支援ツールの利用者は、前記ユーザインタフェース部を通じて、前記サンプル情報と、前記関連付け情報と、前記アクセスログ情報とから、

1つ以上の情報を用いてポリシーの原案を作成し、当該ポリシー原案を元に必要に応じて更に修正を加え、修正後のポリシーを保存することで、前記ポリシー情報を設定することを特徴とするポリシー設定支援ツール。

【請求項 3】

コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、前記ポリシー情報の維持に要する作業負荷を軽減するためのポリシー設定支援ツールであって、

アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、当該差分検出部による検出結果からポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による目視確認および前記ポリシーの更新処理をするためのユーザインタフェース部とから構成されることを特徴とするポリシー設定支援ツール。

【請求項 4】

請求項 3 記載のポリシー設定支援ツールであって、

前記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、前記ユーザインタフェース部を通じて利用者向けに表示し、

前記ポリシー設定支援ツールの利用者は、前記ユーザインタフェース部を通じて表示される前記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば前記ユーザインタフェース部を通じて必要な修正を加えた上で、前記ポリシー情報を保存することを特徴とするポリシー設定支援ツール。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンピュータシステムが管理する情報資産に対するアクセスを、所定のポリシーに基づいてコントロールするアクセス制御システムにおいて、上記ポリシーの作成および維持に要する作業負荷を軽減する場合に好適なポリシー設

定支援ツールに関する。

【0002】

【従来の技術】

一般のコンピュータシステムでは、マルチユーザ・マルチタスクOSが備えるユーザ認証機構と、該認証結果に基づいたアクセス制御機構を用いて情報その他コンピュータ資源の保護を実現しているケースが多い。具体的には、上記OSが実装された情報処理装置を利用する際に、ユーザは必ず自己のユーザIDとパスワードを入力し、認証を受ける。

【0003】

上記情報処理装置が管理する全てのファイル各々には、ファイル読み出しや書き込み等のアクセスタイプ毎に、ユーザIDとグループIDを用いてアクセス可能なユーザを定義したアクセスコントロールリスト（以下、ポリシーと称す）がセキュリティ属性情報として割り当てられている。

【0004】

ユーザがアプリケーションプログラムを介してファイルへアクセスした場合、上記OSは、アクセス要求元となるユーザのID及び該ユーザが所属するグループのIDを、アクセス対象となるファイルやディレクトリに割り当てられたポリシーと照合し、当該リストに上記ユーザが含まれている場合に限りアクセスを許可するといった制御を行う。

【0005】

また、アクセス要求元の情報として、上記ユーザIDやグループIDだけでなく、例えばアクセス手段となるプログラムの識別子まで確認すれば、より厳密なアクセス制御が可能となる。

【0006】

このようなアクセス制御の方法は、例えば特許文献1に開示されている。ただし、不正アクセスを防止するには、本来の利用目的であるサービス提供や業務遂行の上で必要最小限のアクセスのみ許可されるよう、上記ポリシーを設定しておくことが重要である。

【0007】

その他、特許文献 2 には、セキュリティポリシーの作成に要する時間を短縮するために、複数の雛形のポリシーから自己に見合ったものを選択し、修正しながらポリシーを作成する方法が開示されている。

【 0 0 0 8 】

【特許文献 1】

特開 2 0 0 1 - 3 3 7 8 6 4 号公報

【特許文献 2】

特開 2 0 0 2 - 1 0 8 8 1 8 号公報

【 0 0 0 9 】

【発明が解決しようとする課題】

先に述べたように、情報資産を安全に利用するためには、当該情報への必要最小限のアクセスのみ許可するようにポリシーを定義することが重要である。

【 0 0 1 0 】

しかし、ユーザ ID やグループ ID だけでなく、アクセス手段となるプログラムの識別子まで組み合わせてポリシーを定義することは、厳密なアクセス権チェックができる代わりに、そのポリシー作成に手間がかかる。例えば、どのようなデータにアクセスするかといったソフトウェアの仕様を知らなければ、適切なポリシーは設定できない。

【 0 0 1 1 】

ソフトウェアが複数のプログラムから構成されている場合は、特に難しいと言える。上記特許文献 2 に記載されている方法を用いても、雛形のポリシーを自己に見合ったものに修正するのは全て利用者自身であるため、ソフトウェアの仕様を知らなければ、どこをどのように修正すべきか判断できないケースも発生し得る。

【 0 0 1 2 】

また、プログラムアップデートによるプログラムファイル自体の変更が発生したり、ユーザやグループの登録内容に変更が発生したり、更には情報資産であるファイルやディレクトリが、削除・移動・名称書き換え等により変更されることで、現在のポリシーの記述と一致しなくなれば、適切なアクセス制御ができなく

なるという問題もある。

【0013】

そこで、本発明の第一の目的は、利用するソフトウェアの仕様を知らなくても、コンピュータの利用目的を果たす上で適切なファイルアクセスのみを許可するようにポリシーを設定可能な、ポリシー設定支援ツールを提供することにある。

【0014】

本発明の第二の目的は、アクセス主体となるユーザやプログラムの情報の他、アクセス対象となるファイルやディレクトリ等に変更があった場合でも、簡易な操作により関連するポリシーの設定内容を更新可能な、ポリシー設定支援ツールを提供することにある。

【0015】

【課題を解決するための手段】

上記第一の目的を達成するために、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の作成に要する作業負担を軽減するためのポリシー設定支援ツールであって、当該ポリシー設定支援ツールは、アクセス主体となるサブジェクトの種類毎に用意した情報と、アクセス対象となるオブジェクトの種類毎に用意した情報から、適切なポリシーを作成するものであり、上記サブジェクトの種類毎に用意した情報とは、サブジェクトの種類毎に標準的あるいは推奨のポリシーを記述したサンプル情報と、サブジェクトの正常な動作を記録したアクセスログ情報と、対象のコンピュータシステムにインストールされているサブジェクトのインストール先パス名を含むインストール情報とからなり、上記オブジェクトの種類毎に用意した情報とは、オブジェクトの種類毎にアクセス手段として利用される頻度の高いサブジェクトの情報を記述した関連付け情報とからなり、更に上記ポリシー設定支援ツールは、上記サブジェクトの動作を監視して上記アクセスログ情報に記録するためのアクセス監視部と、上記サンプル情報と上記インストール情報とを照合して差分を検出する差分検出部と、上記サンプル情報と上記関連付け情報と上記差分検出部による検出結果とからポリシーの原案を作成するポリシー生成部と、ポリシーの原案を表示して利用者による更なるポリシー

の修正および保存をするためのユーザインタフェース部とから構成されることを特徴としている。

【0016】

上記ポリシー設定支援ツールによれば、例えばソフトウェアの種類毎にサンプルとなるポリシーが提供され、且つ対象のコンピュータシステムに適合したポリシーの原案まで自動的に作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

【0017】

また、本発明は、上記ポリシー設定支援ツールにおいて、当該ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて、上記サンプル情報と、上記関連付け情報と、上記アクセスログ情報とから、1つ以上の情報を用いてポリシーの原案を作成し、当該ポリシー原案を元に必要に応じて更に修正を加え、修正後のポリシーを保存することで、上記ポリシー情報を設定することを特徴としている。

【0018】

これにより、上記サンプルとなるポリシーが用意されていない場合でも、上記関連付け情報やアクセスログ情報からポリシーの原案が作成できるので、利用者はソフトウェアの仕様を知らなくても、適切なポリシーが容易に設定可能となる。

【0019】

また、本発明は、コンピュータが管理する資産をポリシー情報に基づいてアクセス制御する機構を備えたコンピュータシステムにおいて、上記ポリシー情報の維持に要する作業負荷を軽減するためのポリシー設定支援ツールであって、アクセス対象となるオブジェクトならびにアクセス主体となるサブジェクトに関する最新情報と、当該最新情報と設定済みのポリシーの内容とを照合しながら更新すべき項目を検出するための差分検出部と、当該差分検出部による検出結果の表示処理と、利用者による目視確認および上記ポリシーの更新処理をするためのユーザインタフェース部とから構成されることを特徴としている。

【0020】

これにより、アクセス主体となるサブジェクトの情報や、アクセス対象となるオブジェクトに変更があった場合でも、更新すべき項目を自動的に検出して表示できるので、簡易な操作で関連するポリシーの更新が可能となる。

【0021】

また、本発明は、上記ポリシー設定支援ツールにおいて、上記差分検出部による検出処理は、定期的に、あるいは利用者からの要求を受けた時点で実行されるものであり、差分を検出した場合には、当該差分情報を、上記ユーザインタフェース部を通じて利用者向けに表示し、上記ポリシー設定支援ツールの利用者は、上記ユーザインタフェース部を通じて表示される上記差分情報を目視で確認し、当該表示通りに更新すべきかどうかを判断し、更新すべきであれば上記ユーザインタフェース部を通じて必要な修正を加えた上で、上記ポリシー情報を保存することを特徴としている。

【0022】

これにより、利用者は上記ユーザインタフェース部を通じて、差分情報の確認と、ポリシーの修正および保存まで、ポリシーの更新に必要な処理を全て行うことができる。

【0023】

また、定期的な差分検出処理も可能とすることで、利用者が自ら上記差分検出部に対して要求を出さなくても差分情報を取得できるようになるため、無効なポリシー記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

【0024】

【発明の実施の形態】

以下、図を用いて本発明の実施の一形態を説明する。

【0025】

図1は、本実施形態のポリシー設定支援ツールの一構成例である。ポリシー設定支援ツール100は、ユーザインタフェース部101と、ポリシー生成部102、アクセス監視部103、差分検出部104、インストール情報105、関連付け情報106、サンプル情報107、アクセスログ108から構成される。

【 0 0 2 6 】

1 1 0 はアクセス制御部であり、サブジェクト 1 1 1 からオブジェクト 1 1 2 へのアクセスの可否をポリシー情報 1 2 0 の記述内容に従って判定し、ポリシーに合致したアクセスのみ許可し、ポリシー違反のアクセスであれば上記サブジェクト 1 1 1 にエラーを返すといった処理を行う。

【 0 0 2 7 】

このようなアクセス制御は、一般的なオペレーティングシステム（OS）でも標準で備えているが、それらが参照するポリシー情報の多くは、オブジェクトへアクセス可能なサブジェクトを、ユーザやグループの識別子を用いて指定したものである。

【 0 0 2 8 】

これに対して、本実施形態のポリシー設定支援ツールが扱うポリシー情報とは、ユーザやグループの識別子だけでなく、少なくともアクセス手段として用いるプログラムの情報を組み合わせてアクセス権を指定したものである。

【 0 0 2 9 】

なお、サブジェクト情報 1 1 3 は、本実施例においてはインストールされているプログラムファイル群や、登録されているユーザ・グループに関する情報を指す。

【 0 0 3 0 】

上記ポリシー設定支援ツール 1 0 0 は、上記各種情報 1 0 5 ～ 1 0 7 や、上記サブジェクト 1 1 1 からオブジェクト 1 1 2 へのアクセスを記録したアクセスログ 1 0 8 を利用しながらポリシー情報 1 2 0 の設定作業を容易にするものである。また、上記サブジェクト情報 1 1 3 を参照しながら、ポリシーの更新作業を容易にするものでもある。

【 0 0 3 1 】

図 2 は、上記ポリシー設定支援ツール 1 0 0 を利用するために必要なシステムの一例を示したものである。図 2 において、情報処理装置 2 0 0 は、中央演算処理装置 CPU 2 0 1 a と、主記憶 2 0 2 a、外部記憶装置 2 0 3 a、入力装置 2 0 4、表示部 2 0 5、LAN コントローラ 2 0 6 a が、バスなどの通信線（バス

という) 207a に接続することで形成されている。

【0032】

図1にて示したオブジェクト112や、サブジェクト情報113、ポリシー情報120は、上記外部記憶装置203aに格納され、必要に応じて主記憶202aの領域に読み出して利用される。

【0033】

また、上記サブジェクト111やアクセス制御部110は、主記憶202aにロードされ、実行可能プログラムとして上記CPU201aによって処理されるものである。特にアクセス制御部110は、オペレーティングシステム(OS)の一部、あるいはOSに組み込み可能なプログラムとして処理される。

【0034】

同様に、上記ポリシー設定支援ツール100も、主記憶202aにロードされ、上記CPU201aによって処理されるものである。

【0035】

また、ポリシー設定支援ツール100のうち、ユーザインタフェース部101は、上記表示部205にユーザインタフェースを表示し、入力装置204を介して入力されるデータやコマンドに応じて各種処理を実行する。

【0036】

また、インストール情報105や、関連付け情報106、サンプル情報107、アクセスログ108については、外部記憶装置203aに格納しておき、必要に応じて主記憶202aの領域に読み出して利用してもよい。

【0037】

ここまでは、情報処理装置200にて利用されるポリシー情報120を、上記ポリシー設定支援ツール100により設定および更新するために必要なシステム構成である。

【0038】

次に、例えば入力装置204や表示部205をもたないサーバ210におけるポリシー設定および更新処理を、上記情報処理装置200から行うためのシステム構成について説明する。

【 0 0 3 9 】

サーバ 2 1 0 は、CPU 2 0 1 b、主記憶 2 0 2 b、外部記憶装置 2 0 3 b の他に、LAN コントローラ 2 0 6 b をバス 2 0 7 b に接続することで形成される。LAN コントローラ 2 0 6 は、主記憶 2 0 2 にロードされて実行中のプログラムが、ネットワーク 2 2 0 を介して他のネットワークノードとデータを交換するために利用する装置である。

【 0 0 4 0 】

上記アクセス制御部 1 1 0 が、サーバ 2 1 0 の OS あるいは OS に組み込み可能なプログラムとして主記憶 2 0 2 b にロードされて CPU 2 0 1 b により処理され、同じく主記憶 2 0 2 b にロードされて CPU 2 0 1 b により処理されるプログラムをサブジェクト 1 1 1 とみなし、当該サブジェクトからオブジェクト 1 1 2 へのアクセスを制御することを前提とし、以下説明する。

【 0 0 4 1 】

なお、ポリシー情報 1 2 0 やオブジェクト 1 1 2、サブジェクト情報 1 1 3 は、外部記憶装置 2 0 3 b に格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

【 0 0 4 2 】

このようなシステム構成において、本実施形態のポリシー設定支援ツール 1 0 0 を利用する場合は、少なくとも入力装置 2 0 4 と表示部 2 0 5 の利用を前提とする上記ユーザインタフェース部 1 0 1 を、情報処理装置 2 0 0 側の主記憶 2 0 2 a にて実行させ、それ以外のポリシー生成部 1 0 2、アクセス監視部 1 0 3、差分検出部 1 0 4 はサーバ 2 1 0 側の主記憶 2 0 2 b にて実行させ、互いにネットワーク 2 2 0 を介してデータ交換を行いながら各種処理を実行する。

【 0 0 4 3 】

また、インストール情報 1 0 5 や、関連付け情報 1 0 6、サンプル情報 1 0 7、アクセスログ 1 0 8 については、外部記憶装置 2 0 3 b に格納してもよいし、他のネットワークノードと共有可能な外部記憶装置を別途用意して格納してもよい。

【 0 0 4 4 】

これにより、遠隔地にある複数のサーバに対しても、同一の情報処理装置からポリシーの設定および更新が可能となる。

【0 0 4 5】

図5は、上記ポリシー情報120の一例を示したものである。上述のように、本実施形態のポリシー設定支援ツール100が扱うポリシー情報とは、オブジェクトへアクセス可能なサブジェクトを、プログラム名とユーザ・グループの識別子との組み合わせで指定したものである。

【0 0 4 6】

図5の例で言うと、ユーザ名”www”の権限で実行しているプログラム”/as/wserv.exe”のみ、オブジェクト名”/www/pub/*”で示されるファイル群に対してアクセス”R”（読み出し）を許可するといったものである。図5における特徴値とは、プログラムの特徴を表す数値のことであり、例えばプログラムファイルのサイズや、ハッシュ関数を用いて算出した値を利用する。

【0 0 4 7】

アクセス発生時に、上記アクセス制御部110が特徴値を確認することで、不当に改ざんされたプログラムによるアクセスからオブジェクトを保護することも可能となる。また、図5における時間とは、アクセスを許可する時間帯のことであり、特に指定がない場合は、終日アクセス可能となるよう”00:00-24:00”と設定する。

【0 0 4 8】

また、図5におけるソフトウェア名称とは、上記プログラムが構成するソフトウェアに付けられた名称である。これは、利用者がポリシーを編集する際に、ソフトウェア名称を用いてプログラムを指定可能とすることを目的に登録されたものであり、上記アクセス制御部110によるアクセス権チェックの際には無視される情報である。

【0 0 4 9】

図3は、上記インストール情報105や、関連付け情報106、サンプル情報107、アクセスログ108の一例を示したものである。インストール情報105とは、上記サブジェクト情報に格納されているプログラムに関する情報を、ソ

フトウェアの種類毎に分類して管理するためのものである。

【 0 0 5 0 】

その内容は、ソフトウェア名称と、実行ファイル名称、当該実行ファイルのインストール先となるディレクトリ名、更には当該ソフトウェアをアンインストールする際に実行すべきアンインストールプログラムの名称といった情報からなる。

【 0 0 5 1 】

図 3 の例では、” M 3 メール 3.0 ” というソフトウェア名称がインストールされており、その実体となる実行ファイルが” M3MAIL.exe ” であり、当該実行ファイルのインストール先が” /m3/ ” ディレクトリの下であり、アンインストールプログラムの名称が” /m3/uninstall.exe ” であることを表している。

【 0 0 5 2 】

このような情報は、一般的なオペレーティングシステム（OS）でも管理している場合が多いことから、本実施形態のポリシー設定支援ツール 1 0 0 が独自に管理せずに、OS が管理しているインストール情報を利用することも考えられる。

【 0 0 5 3 】

次に、関連付け情報 1 0 6 とは、オブジェクト 1 1 2 をアクセスする際に、そのアクセス手段として利用される頻度の高いプログラムの情報を、オブジェクトの種類毎に管理するためのものである。図 3 の例では、ファイル名の拡張子が” txt ” のオブジェクトへアクセスする際には、利用者からの特別な指示がない限り、実行ファイル名称が” /tools/gpad.exe ” のプログラムを利用することを意味している。

【 0 0 5 4 】

このような情報も、一般的な OS が管理している場合が多いことから、本実施形態のポリシー設定支援ツール 1 0 0 が独自に管理せずに、OS が管理している関連付け情報を利用することも考えられる。

【 0 0 5 5 】

3 つ目に、サンプル情報 1 0 7 とは、ソフトウェアの種類毎に標準的な、ある

いは推奨のポリシー情報を記述したものである。図 3 の例では、ソフトウェア名称が” アタッチサーバ2.0” というプログラムを利用するならば、オブジェクト名が” /www/pub/*” で表されるファイルに対しては、実行ファイル名称が” /as/wserv.exe” のプログラムが、ユーザ・グループ名が” www” の権限で実行している場合に限り、アクセスタイプ” R” つまり読み出しのみ許可することを表している。

【 0 0 5 6 】

4 つ目に、アクセスログ 1 0 8 とは、上記サブジェクト 1 1 1 からオブジェクト 1 1 2 へのアクセスを、上記アクセス監視部 1 0 3 により監視して、当該アクセス内容を記録したものである。図 3 に示したアクセスログの一行目の例では、オブジェクト名に示されるファイル” /datafile.db” に対して、サブジェクト情報として示されているプログラム名” /db/hdbr.exe” のプログラムがユーザ名” system” の権限によって、アクセスタイプに示されるアクセス” RW” （読み出しと書き込み）を実行したことを表している。

【 0 0 5 7 】

図 4 は、ポリシー設定支援ツール 1 0 0 のユーザインタフェース部 1 0 1 が、当該ツールの利用者向けに提供するポリシー設定画面 4 0 0 の一例を示すものである。利用者は、図 2 の表示部 2 0 5 に表示された上記ポリシー設定画面 4 0 0 を利用することにより、ポリシー情報 1 2 0 の設定や更新、参照といった各種編集作業が可能となる。

【 0 0 5 8 】

ポリシー設定画面 4 0 0 のうち、4 1 0 はポリシー情報 1 2 0 に現在登録されているポリシー一覧を表示するボックスである。当該ポリシー表示ボックス 4 1 0 は、アクセス対象となるオブジェクト名と、アクセス主体となるサブジェクト情報と、許可されたアクセスタイプと、アクセス可能な時間帯を表す情報から構成される。

【 0 0 5 9 】

図 4 （a）の例では、サブジェクト情報として、ソフトウェアの名称を表示している。これは、図 3 で示したインストール情報 1 0 5 に格納されているソフト

ウェア名称と同じものである。これにより、利用者にとってポリシーの概要を把握し易くなるという効果が期待できる。

【 0 0 6 0 】

4 1 1 は、ポリシーの表示を切り替えるための切替ボタンであり、利用者が当該切替ボタン 4 1 1 a を押下すると、図 4 (b) に示すように、サブジェクト情報の表示が、プログラム名とプログラムファイルの特徴値、およびユーザ・グループ名といった、より詳細なものへと切り替わる。反対に、図 4 (b) の切替ボタン 4 1 1 b を押下すると、図 4 (a) の 4 1 0 a のような、ソフトウェア名称だけの表示へと切り替わる。

【 0 0 6 1 】

このようなサブジェクト情報の表示切り替えを可能とするためには、上記図 3 に示したインストール情報 1 0 5 に格納されたソフトウェア名称を、図 5 に示すようにポリシー情報 1 2 0 に対しても識別子として登録し、各プログラムとソフトウェア名称の対応関係を保持しておけばよい。

【 0 0 6 2 】

または、上記ソフトウェア名称の代わりに、ユニークな識別番号を各ソフトウェアに対して割り当てて、上記インストール情報 1 0 5 と上記ポリシー情報 1 2 0 の両方に登録してもよい。

【 0 0 6 3 】

また、複数のプログラムファイルから構成されるソフトウェアであれば、それらプログラムファイルには全て同一の識別番号あるいは識別子を、上記ポリシー情報 1 2 0 に登録する。多くの場合、それらプログラムファイルの格納先は共通のディレクトリ下であることから、共通のディレクトリ下にあるプログラムファイルに対して同一のソフトウェア識別番号あるいは識別子を割り当てればよい。

【 0 0 6 4 】

上記ユーザインタフェース部 1 0 1 は、上記切替ボタン 4 1 1 が押下される度に、ポリシー情報 1 2 0 を参照しながら上記ポリシー表示ボックス 4 1 0 内のサブジェクト情報の表示内容を切り替えることになる。

【 0 0 6 5 】

4 2 0 は、ポリシーを生成、変更するための編集用ボックスである。4 2 1 は、編集用ボックス 4 2 0 に記述したポリシーを上記ポリシー表示ボックス 4 1 0 に追加して、ポリシー情報 1 2 0 に保存するための追加ボタンである。

【0 0 6 6】

上記編集用ボックス 4 2 0 には、オブジェクト名とサブジェクト情報、アクセスタイプ、時間を指定できるが、これら項目を利用者が一つ一つ入力してもよいし、後述するように簡易設定ボタン 4 3 0 を利用して指定することもできる。

【0 0 6 7】

また、上記ポリシー表示ボックス 4 1 0 からポリシーを選択すると、上記ユーザインタフェース部 1 0 1 が、当該ポリシーを上記編集用ボックス 4 2 0 に表示するので、既に登録済みのポリシーを一部変更する際には、上記ポリシー表示ボックス 4 1 0 に表示されたポリシーから変更したいものを選択して上記編集用ボックス 4 2 0 に表示し、必要な修正を加えてから上記追加ボタン 4 2 1 を押下すればよい。

【0 0 6 8】

上記ポリシー設定画面 4 0 0 には、上記簡易設定ボタン 4 3 0 の他、サンプル登録ボタン 4 3 1、更新ボタン 4 3 2、削除ボタン 4 3 3、終了ボタン 4 3 4 がある。以下、これらボタンの意味について説明する。

【0 0 6 9】

簡易設定ボタン 4 3 0 は、上記サンプル情報 1 0 7 や、関連付け情報 1 0 6、アクセスログ 1 0 8 等を利用して、ポリシー原案を自動生成する際に押下するボタンである。当該処理については後述する。

【0 0 7 0】

サンプル登録ボタン 4 3 1 は、上記編集用ボックス 4 2 0 の表示内容を上記サンプル情報 1 0 7 に登録し、以後サンプルポリシーとして再利用可能なものとする際に押下するボタンである。

【0 0 7 1】

更新ボタン 4 3 2 は、上記ポリシー情報 1 2 0 に登録されているポリシーを、最新のオブジェクトやサブジェクト情報 1 1 3 に合わせて更新する際に押下する

ボタンである。この処理についても後述する。

【 0 0 7 2 】

登録済みのポリシーを一部削除したい場合には、上記ポリシー表示ボックス 4 1 0 に表示されたポリシーから削除したいものを選択して、削除ボタン 4 3 3 を押下する。また、ポリシー編集作業を終了する場合には、終了ボタン 4 3 4 を押下する。

【 0 0 7 3 】

図 6 は、上記簡易設定ボタン 4 3 0 を押下したときに、図 2 の表示部 2 0 5 に出現する簡易設定インタフェースの一例を示したものである。利用者は、簡易設定インタフェース 6 0 0 を通じて、上記サンプル情報 1 0 7 を利用したポリシー原案作成や、上記関連付け情報 1 0 6 を利用したポリシー原案作成、更には上記アクセスログ 1 0 8 を利用したポリシー原案作成を実行することができる。

【 0 0 7 4 】

図 6 の 6 0 1 は、インストールされているソフトウェア一覧表示ボックスであり、上記ユーザインタフェース部 1 0 1 が、上記インストール情報 1 0 5 およびサンプル情報 1 0 7 を参照して、現在インストールされていて且つサンプルポリシーが用意されているソフトウェアのみを表示する。

【 0 0 7 5 】

利用者が、これらソフトウェアのサンプルポリシーを利用してポリシーの原案を作成する場合には、各ソフトウェアに対応したチェックボックス 6 0 3 a にチェックを付けて、原案作成ボタン 6 0 8 を押下すればよい。

【 0 0 7 6 】

図 6 の 6 0 2 は、特定のソフトウェアとの関連付けがされているファイル拡張子一覧表示ボックスであり、上記ユーザインタフェース部 1 0 1 が上記関連付け情報 1 0 6 を参照して表示する。当該関連付け情報を利用してポリシーの原案を作成する場合には、各拡張子に対応したチェックボックス 6 0 3 b にチェックを付けて、原案作成ボタン 6 0 8 を押下すればよい。

【 0 0 7 7 】

図 6 の 6 0 5 は、監視したいプログラムを指定するための入力ボックスであり

、ここにプログラム名を入力して開始ボタン 6 0 6 を押下すると、上記アクセス監視部によるアクセス監視と上記アクセスログ 1 0 8 への記録を開始する。終了ボタンを押下すると、上記アクセス監視とアクセスログ記録を終了する。

【 0 0 7 8 】

その後で、上記原案作成ボタン 6 0 8 を押下すると、アクセスログ 1 0 8 を利用してポリシー原案を作成することができる。なお、上記プログラムの指定は、プログラムファイル名の代わりに、ソフトウェアの名称で指定できるものでもよい。

【 0 0 7 9 】

上記のように作成されたポリシー原案は、上記ユーザインタフェース部 1 0 1 の処理により、図 4 の編集用ボックス 4 2 0 に表示される。当該ポリシー原案をベースに、利用者が一部修正を加えるなど、編集作業を行ってから上記追加ボタン 4 2 1 を押下すると、当該編集されたポリシーを上記ポリシー表示ボックス 4 1 0 に追加すると共に、ポリシー情報 1 2 0 にも保存する。

【 0 0 8 0 】

図 6 の 6 0 9 は、キャンセルボタンであり、上記簡易設定インタフェース 6 0 0 の処理を終了して、図 4 のポリシー設定画面 4 0 0 へ戻る際に押下する。

【 0 0 8 1 】

図 7 は、サンプル情報からポリシー原案を生成する処理手順の一例を示したものである。ステップ 7 0 1 は、上記ユーザインタフェース部 1 0 1 へのコマンド入力であり、これは図 6 のソフトウェア一覧表示ボックス 6 0 1 からソフトウェアを選択して、上記原案作成ボタン 6 0 8 を押下することに相当する。

【 0 0 8 2 】

ステップ 7 0 2 では、上記ポリシー生成部 1 0 2 により、上記選択されたソフトウェアに対応するサンプル情報を取得する。ステップ 7 0 3 では、上記差分検出部 1 0 3 により、上記サブジェクト情報 1 1 3 やオブジェクト 1 1 2 を参照して、上記サンプル情報との差分データを作成する。

【 0 0 8 3 】

これは、ソフトウェアのインストール先や、ディレクトリ構成が標準と異なる

場合、上記サンプル情報がそのまま利用できないことがあるためである。ステップ 7 0 4 では、上記ポリシー生成部 1 0 2 により、上記サンプル情報と差分データを基に、対象となる情報処理装置やサーバに相応しいポリシーの原案を生成する。

【 0 0 8 4 】

このとき、アクセス許可されるプログラムの特徴値算出も併せて行う。また、アクセス許可する時間帯については、特に指定がない限り、終日（00:00-24:00）に設定しておく。ステップ 7 0 5 では、上記ユーザインタフェース部 1 0 1 により、上記ポリシーの原案を、上記図 4 の編集用ボックス 4 2 0 に表示する。

【 0 0 8 5 】

ステップ 7 0 6 では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ 7 0 7 では、上記修正後のポリシーを、上記ポリシー情報 1 2 0 へ保存する。このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名その他、ソフトウェア名称も付加して保存する。

【 0 0 8 6 】

次に図 8 を用いて、関連付け情報 1 0 6 を利用したポリシー生成の処理手順の一例を説明する。ステップ 8 0 1 は、上記ユーザインタフェース部 1 0 1 へのコマンド入力であり、これは図 6 のファイル拡張子一覧表示ボックス 6 0 2 から拡張子を選択して、上記原案作成ボタン 6 0 8 を押下することに相当する。

【 0 0 8 7 】

ステップ 8 0 2 では、上記関連付け情報 1 0 6 を参照して、上記利用者が選択した拡張子に関連付けられたプログラムの実行ファイル名称を取得する。ステップ 8 0 3 では、上記ポリシー生成部 1 0 2 により、上記取得した情報を基にポリシーの原案を生成する。

【 0 0 8 8 】

このとき生成されるポリシーの原案は、オブジェクト名と、プログラム名と、プログラムの特徴値と、時間帯のみ指定されており、ユーザ・グループ名やアク

セスタイプは指定していない。ただし、図 2 に示した上記情報処理装置 2 0 0 やサーバ 2 1 0 が利用している OS 自身が、上記アクセス制御部 1 1 0 とは異なる独自のアクセス制御機構を備えている場合はその通りでない。

【 0 0 8 9 】

つまり、当該 OS 独自のアクセス制御機構があれば、各オブジェクトへのアクセス条件として、ユーザ・グループの情報や、アクセスタイプが設定されているはずである。そこで、例えば上記ポリシー生成部 1 0 2 がこれらユーザ・グループの識別子やアクセスタイプを取得して、上記ポリシーの原案に取り込むものであってもよい。

【 0 0 9 0 】

また、同じ拡張子をもつファイルでも、これらユーザ・グループやアクセスタイプが異なるものは、オブジェクト名を区別してそれぞれ個別のポリシーとなるよう原案を作成する。

【 0 0 9 1 】

このようにして生成したポリシー原案は、ステップ 8 0 4 にて上記ユーザインタフェース部 1 0 1 が、上記図 4 の編集用ボックス 4 2 0 に表示する。ステップ 8 0 5 では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

【 0 0 9 2 】

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ 8 0 6 では、上記修正後のポリシーを、上記ポリシー情報 1 2 0 へ保存する。

【 0 0 9 3 】

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名その他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報 1 0 5 より取得する。

【 0 0 9 4 】

次に図 9 を用いて、上記アクセスログ 1 0 8 を利用したポリシー生成処理手順の一例を説明する。ステップ 9 0 1 は、上記ユーザインタフェース部 1 0 1 への

コマンド入力であり、これは図 6 の入力ボックス 6 0 5 にプログラムを指定して、上記開始ボタン 6 0 6 を押下することに相当する。

【0 0 9 5】

ステップ 9 0 2 では、上記アクセス監視部 1 0 3 により、上記指定されたプログラムから発行されるファイルアクセスを監視して、その内容を上記アクセスログ 1 0 8 に記録する。この処理は、上記図 6 の終了ボタン 6 0 7 を押下するまで継続する。

【0 0 9 6】

ステップ 9 0 3 では、上記ポリシー生成部 1 0 2 により、上記アクセスログ 1 0 8 からポリシー原案を生成する。このとき、上記アクセスログ 1 0 8 に記録されたアクセスは、正当なアクセスとして許可されるようにポリシー原案を作成する。

【0 0 9 7】

また、サブジェクトとなるプログラムの特徴値も算出し、上記ポリシー原案に取り入れる。時間帯指定については、特に指定がない限り” 00:00-24:00”（終日）とする。

【0 0 9 8】

このようにして生成したポリシー原案は、ステップ 9 0 4 にて上記ユーザインタフェース部 1 0 1 が、上記図 4 の編集用ボックス 4 2 0 に表示する。ステップ 9 0 5 では、表示されたポリシー原案に対して、利用者自身により必要な修正を加える。

【0 0 9 9】

この修正とは、例えばアクセス許可する時間帯の指定や、ユーザ・グループの指定変更等である。ステップ 9 0 6 では、上記修正後のポリシーを、上記ポリシー情報 1 2 0 へ保存する。

【0 1 0 0】

このとき、サブジェクト情報として、プログラム名、特徴値、ユーザ・グループ名その他、ソフトウェア名称も付加して保存する。当該ソフトウェア名称は、上記インストール情報 1 0 5 より取得する。

【 0 1 0 1 】

以上の図 7 から図 9 の処理を、利用者が必要に応じて繰り返したり、組み合わせたりしながらポリシーを作成することになる。

【 0 1 0 2 】

次に、図 1 0 を用いて上記差分検出部 1 0 4 の処理手順について説明する。これは、上記オブジェクト 1 1 2 やサブジェクト情報 1 1 3 に変更が生じた場合にも、登録済みのポリシー情報 1 2 0 への反映を容易にするための処理である。

【 0 1 0 3 】

ステップ 1 0 0 1 は、例えば上記ユーザインタフェース部 1 0 1 へのコマンド入力であり、これは上記図 4 の更新ボタン 4 3 2 を押下することに相当する。あるいは、図 2 の上記情報処理装置 2 0 0 やサーバ 2 1 0 に搭載された OS が備えるスケジューラ機能等により、差分検出部 1 0 4 の処理を定期的に実行させるものであってもよい。

【 0 1 0 4 】

そして差分が検出された場合には、ポリシーの記述を見直す必要があることを、上記ユーザインタフェース部 1 0 1 を通じて利用者に通知することで、無効なポリシーの記述を放置することなく、常に適切なポリシーに基づくアクセス制御が可能となる。

【 0 1 0 5 】

ステップ 1 0 0 2 では、差分検出部 1 0 4 が上記ポリシー情報 1 2 0 を参照し、当該ポリシー情報 1 2 0 に登録されているオブジェクト名とサブジェクト情報を取得する。ステップ 1 0 0 3 では、オブジェクトとサブジェクトに関する最新情報を、上記オブジェクト 1 1 2 とサブジェクト情報 1 1 3 とから取得し、上記ポリシー情報 1 2 0 の内容と照合する。

【 0 1 0 6 】

ステップ 1 0 0 4 では、上記照合処理の結果、更新の必要があると思われるポリシーについてはその内容を上記ユーザインタフェース部 1 0 1 に渡し、図 1 1 に示すように、上記編集用ボックス 4 2 0 に表示する。このとき、変更のあった部分が他よりも目立つよう強調表示する。

【 0 1 0 7 】

利用者は、当該変更内容を目視で確認し（ステップ 1 0 0 5）、更新しても問題ないと判断するならば、必要な修正を加えた上で、図 1 1 の更新ボタン 4 2 2 を押下することで、正式に上記ポリシー情報 1 2 0 の内容を更新できる（ステップ 1 0 0 6）。仮に、プログラムのアップデートをした覚えがないのに、プログラムの特徴値に変更があった場合は、プログラムファイルの不当な改ざんが発生した可能性もあると考えられ、この場合は、利用者はポリシーの更新をせずに上記プログラムファイル改ざんの原因を確認すればよい。

【 0 1 0 8 】

以上述べたように、本実施形態によれば、ソフトウェアの仕様を詳しく知らなくても、ソフトウェアの種類毎に用意したサンプルポリシーや、関連づけ情報、ソフトウェアのアクセスログを利用することで、適切なポリシーを短時間に作成することができる。

【 0 1 0 9 】

また、オブジェクトやサブジェクトの情報に変更があった場合でも、変更すべきポリシーの部分が利用者にとって容易に判るよう表示でき、且つ簡易な操作で更新可能であることから、常に適切なポリシー情報に基づくアクセス制御が可能となる。

【 0 1 1 0 】**【発明の効果】**

本発明によれば、ポリシーの作成および維持に要する作業負荷を軽減することが可能になる。

【図面の簡単な説明】

【図 1】 本実施形態におけるポリシー設定支援ツールの一構成例を示す図。

【図 2】 ポリシー設定支援ツールを利用するためのコンピュータシステムの一構成例を示す図。

【図 3】 インストール情報と関連付け情報とサンプル情報とアクセスログの一例を示す図。

【図 4】 本実施形態において、ポリシー設定画面 4 0 0 の一例を示す図。

【図 5】 本実施形態において、ポリシー情報 120 の一例を示す図。

【図 6】 本実施形態において、簡易設定インタフェース 600 の一例を示す図。

【図 7】 サンプル情報 107 からポリシーを作成する処理のフローチャートを示す図。

【図 8】 関連付け情報 106 からポリシーを作成する処理のフローチャートを示す図。

【図 9】 アクセスログ 108 からポリシーを作成する処理のフローチャートを示す図。

【図 10】 差分検出部 104 によるポリシー更新処理のフローチャートを示す図。

【図 11】 編集用ボックス 420 に表示するポリシーの変更情報の一例を示す図。

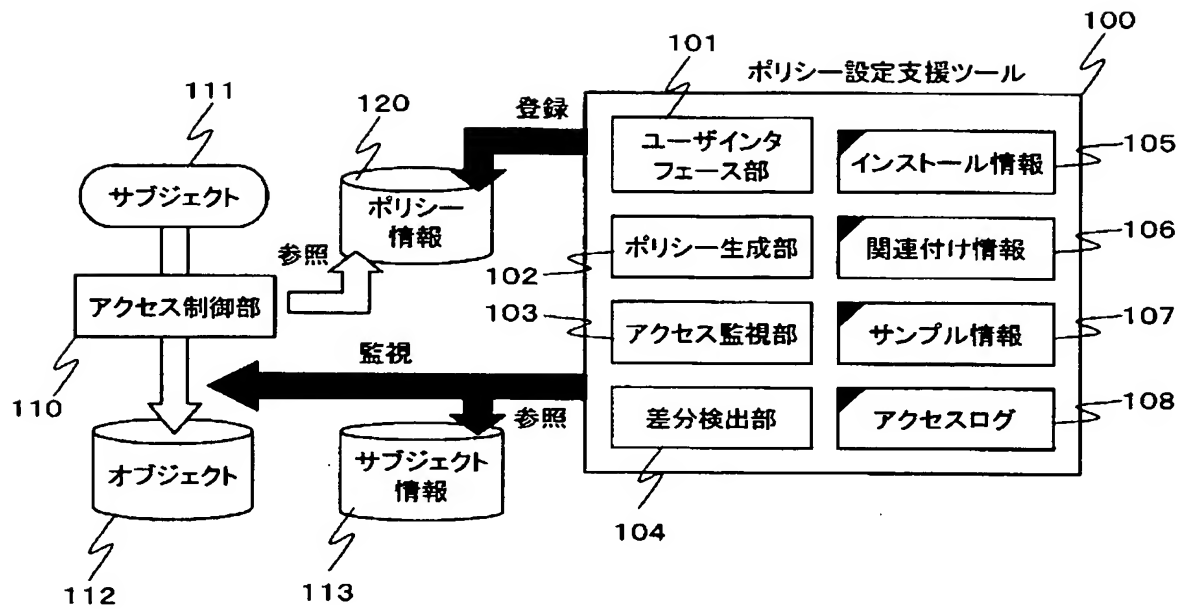
【符号の説明】

100…ポリシー設定支援ツール、101…ユーザインタフェース部、102…ポリシー生成部、103…アクセス監視部、104…差分検出部、105…インストール情報、106…関連付け情報、107…サンプル情報、108…アクセスログ、110…アクセス制御部、111…サブジェクト、112…オブジェクト、113…サブジェクト情報、120…ポリシー情報、200…情報処理装置、201…CPU、202…主記憶、203…外部記憶装置、204…入力装置、205…表示部、206…LANコントローラ、210…サーバ、220…ネットワーク、400…ポリシー設定画面、410…ポリシー表示ボックス、411…切替ボタン、420…編集用ボックス、421…追加ボタン、422…更新ボタン、430…簡易設定ボタン、431…サンプル登録ボタン、432…更新ボタン、433…削除ボタン、434…終了ボタン、600…簡易設定インタフェース、601…ソフトウェア一覧表示ボックス、602…ファイル拡張子一覧表示ボックス、603…チェックボックス、605…入力ボックス、606…開始ボタン、607…終了ボタン、608…原案作成ボタン、609…キャンセルボタン。

【書類名】 図面

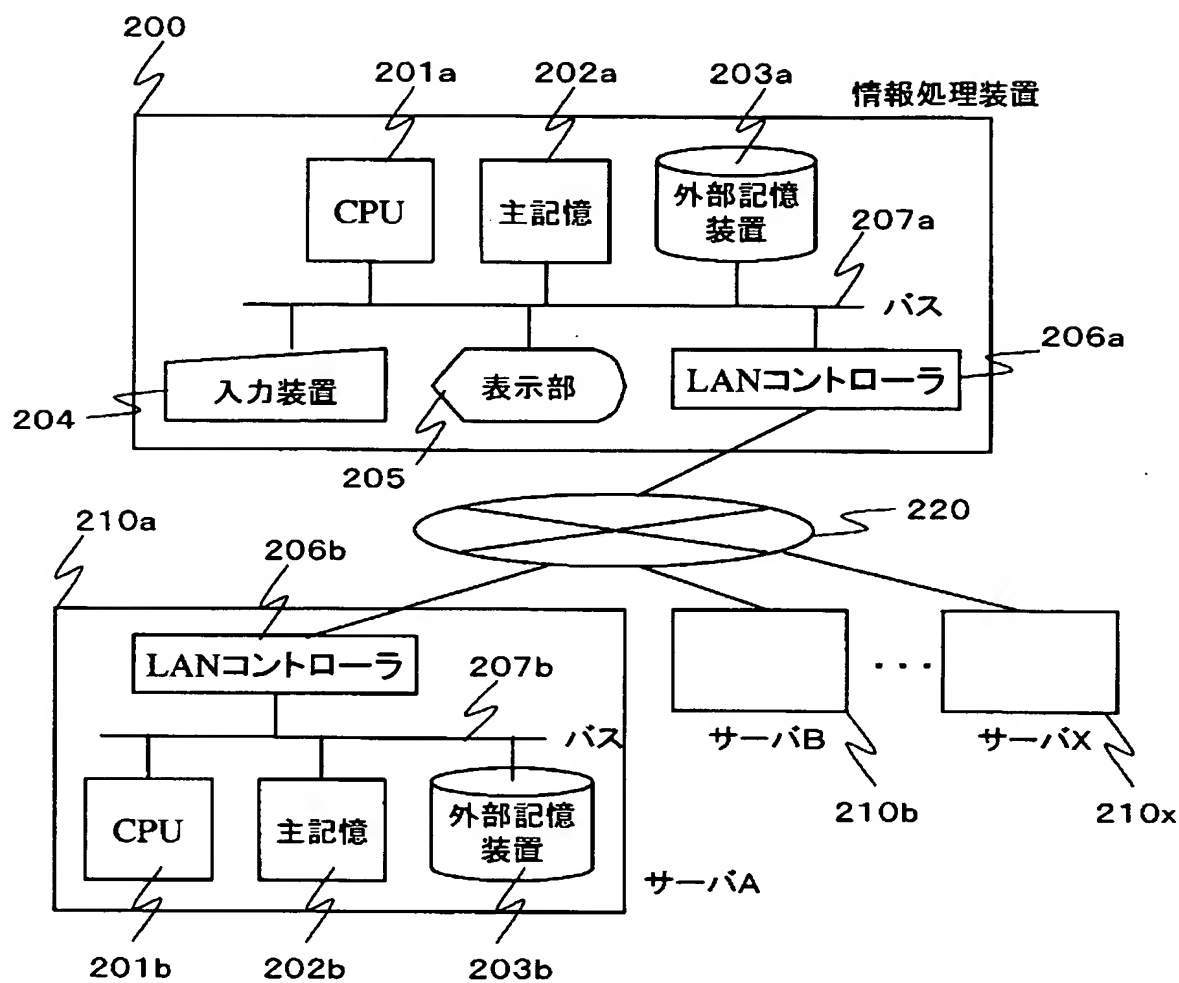
【図 1】

図 1



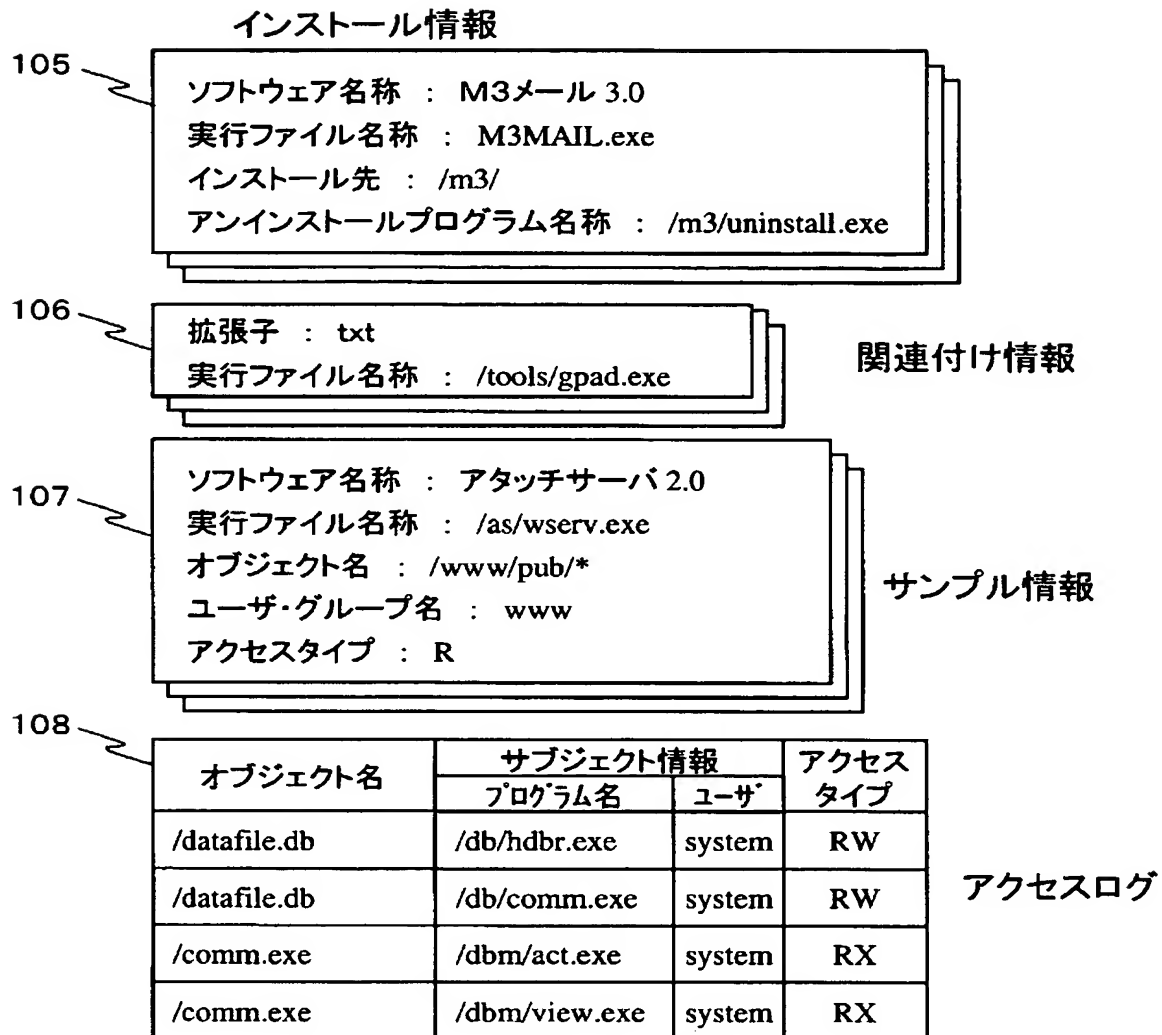
【図 2】

図 2



【図 3】

図 3



【図 4】

図 4

(a)

400

411a

表示	オブジェクト名	サブジェクト情報			アクセス タイプ	時間
<input checked="" type="checkbox"/>	/www/pub/*	アタッチサーバ 2.0			R	00:00-24:00
<input checked="" type="checkbox"/>	*.txt	ギガパッド 1.0			RW	00:00-24:00
<input checked="" type="checkbox"/>	/db/datafile.db	Hi-DBマネージャ 5.0			RWD	00:00-24:00
<input checked="" type="checkbox"/>	/mail/satou/*	M3メール 3.0			RWDX	00:00-24:00

410a

420

421

	オブジェクト名	サブジェクト情報			アクセス タイプ	時間
		プログラム名	特徴値	ユーザ		
<input type="checkbox"/>	/www/custom/*	/as/reg.exe	24680	www	RW	08:00-22:00
						00:00-24:00

430

431

432

433

434

簡易設定

サンプル登録

更新

削除

終了

(b)

410b

411b

表示	オブジェクト名	サブジェクト情報			アクセス タイプ	時間
		プログラム名	特徴値	ユーザ		
<input type="checkbox"/>	/www/pub/*	/as/wserv.exe	12345	www	R	00:00-24:00
<input type="checkbox"/>	*.txt	/tools/gpad.exe	13579	users	RW	00:00-24:00
<input type="checkbox"/>	/datafile.db	/db/hdbr.exe	98765	system	RW	00:00-24:00
		/db/comm.exe	43210	system	RWD	00:00-24:00
<input type="checkbox"/>	/mail/satou/*	/m3/m3mail.exe	91827	satou	RWDX	00:00-24:00

【図 5】

図 5

120

オブジェクト名	サブジェクト情報				アクセス タイプ	時間
	プログラム名	特徴値	ユーザ	ソフトウェア名称		
/www/pub/*	/as/wserv.exe	12345	www	アタッチサーバ2.0	R	00:00-24:00
*.txt	/tools/gpad.exe	13579	users	ギガパッド1.0	RW	00:00-24:00
/datafile.db	/db/hdbr.exe	98765	system	Hi-DBマネージャ5.0	RW	00:00-24:00
	/db/comm.exe	43210	system	Hi-DBマネージャ5.0	RWD	00:00-24:00
/mail/satou/*	/m3/m3mail.exe	91827	satou	M3メール3.0	RWDX	00:00-24:00

【図 6】

図 6

600

サンプルを利用したいものにチェック ☒ を付けて下さい

603a	<input checked="" type="checkbox"/>	アタッチサーバ 2.0	601
	<input checked="" type="checkbox"/>	ギガパッド 1.0	
	<input checked="" type="checkbox"/>	Hi-DBマネージャ 5.0	
	<input checked="" type="checkbox"/>	M3メール 3.0	

関連付けを利用したいものにチェック ☒ を付けて下さい

603b	<input checked="" type="checkbox"/>	txt	602
	<input type="checkbox"/>	doc	
	<input type="checkbox"/>	ppt	
	<input type="checkbox"/>	cca	

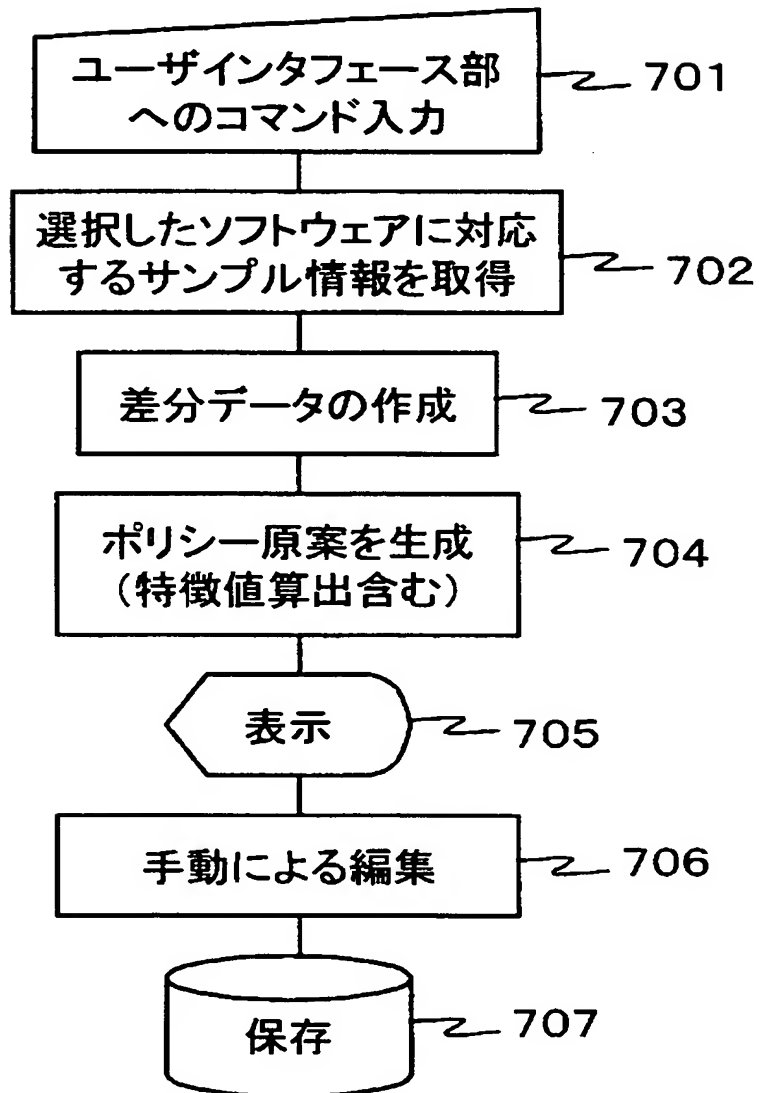
監視したいプログラムを指定して下さい。

605 606 607

608 609

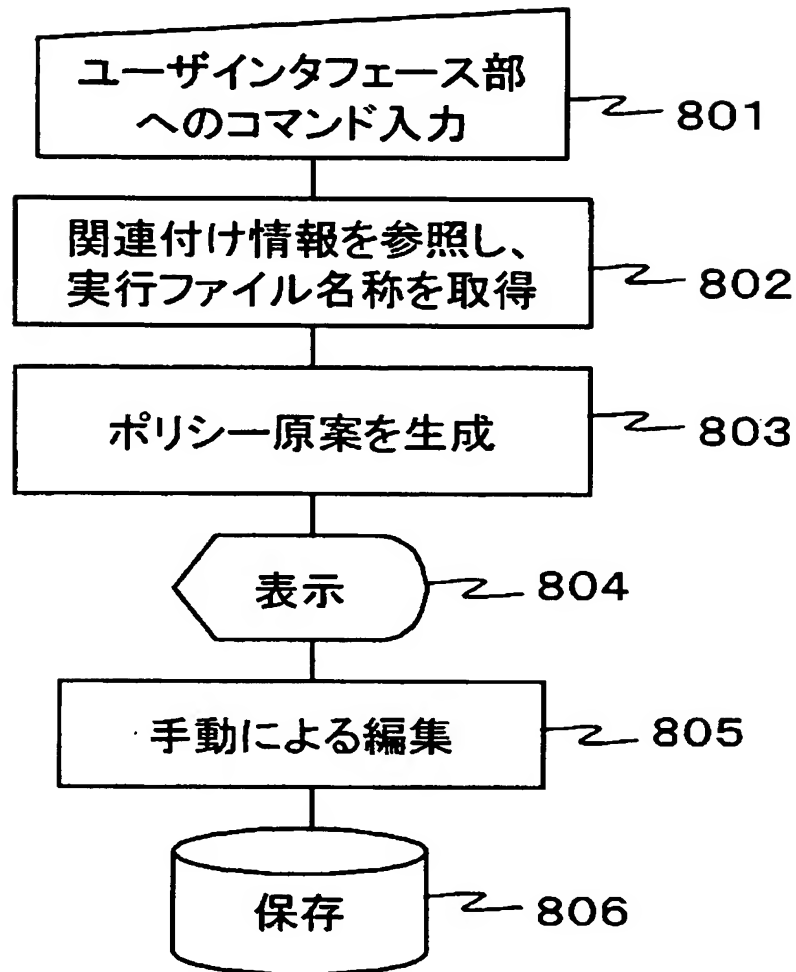
【図 7】

図 7

サンプル情報からポリシー
を作成する手順

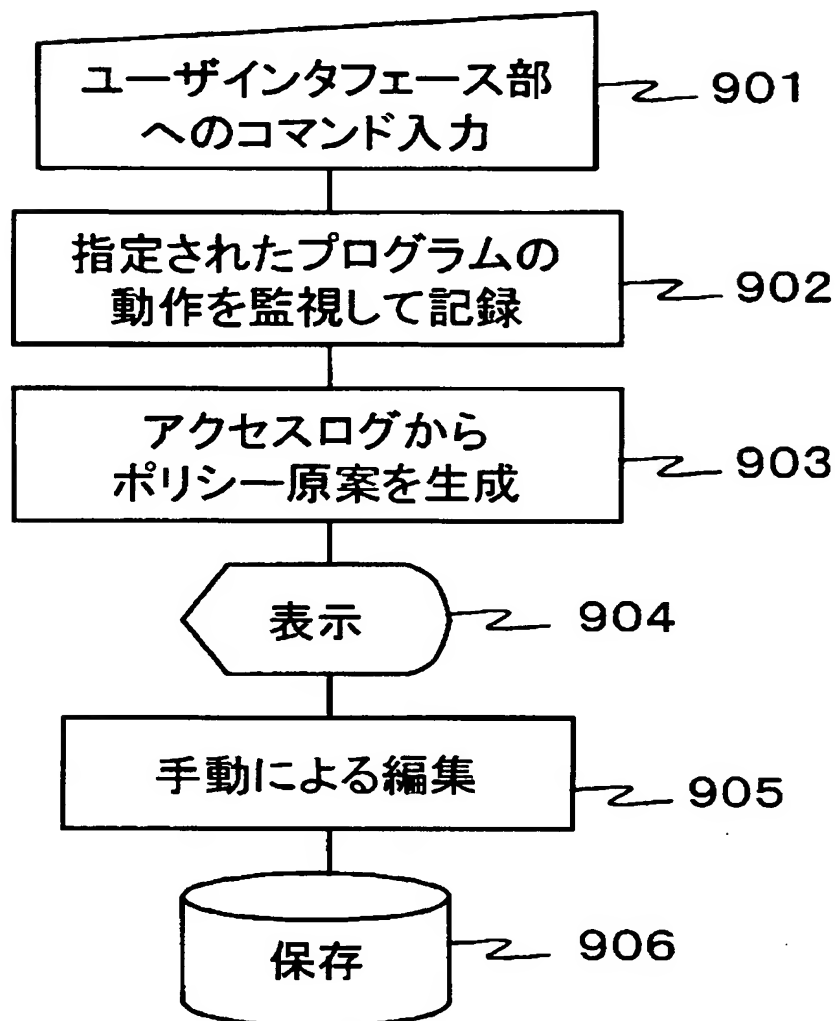
【図 8】

図 8

関連づけ情報からポリシー
を作成する手順

【図 9】

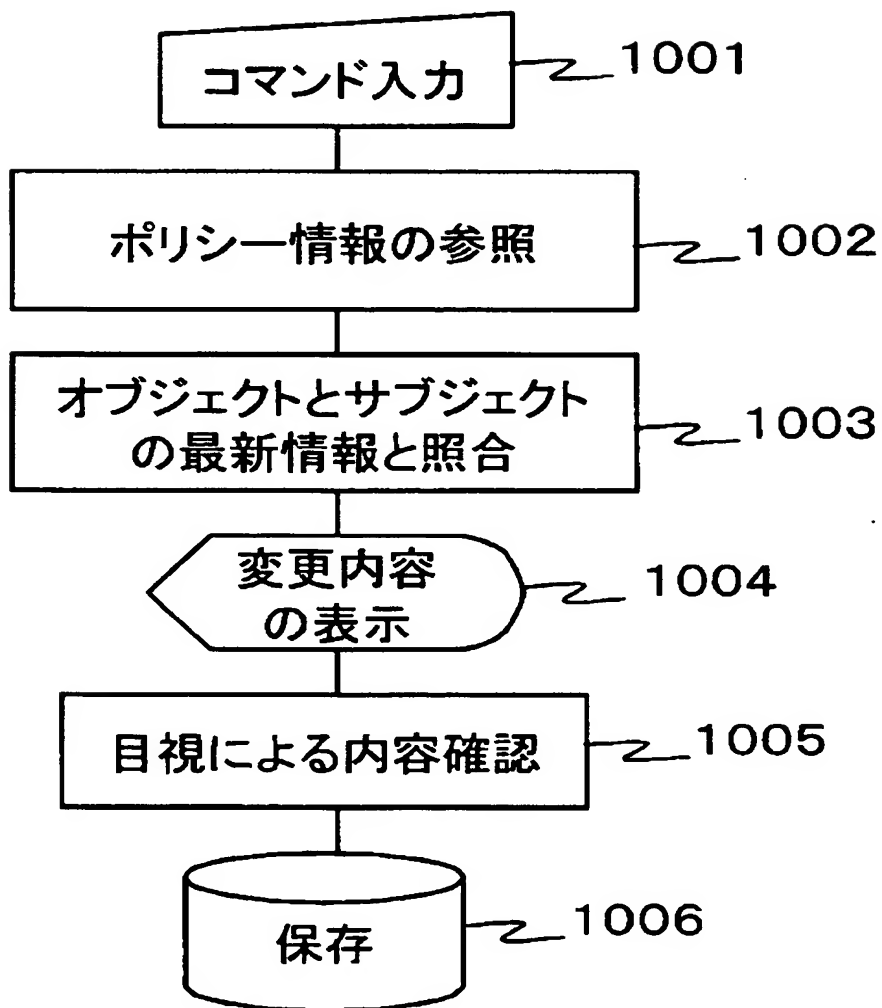
図 9

アクセスログからポリシー
を作成する手順

【図 10】

図 10

差分検出部の処理



【図 11】

図 11

更新	オブジェクト名	サブジェクト情報			アクセス タイプ	時間	420
		プログラム名	特徴値	ユーザ			
更新	/www/custom/*	/as/reg.exe	991760	www	RW	08:00-22:00	422
更新	/doc/sum.dat は存在しません	rec.exe	54321	users	RWD	00:00-24:00	
更新	/www/custom/*	/as/reg.exe	54321	suzuki は存在しません		:00	
更新	/www/custom/*	/ap/rc.exe は存在しません			RW	00:00-24:00	

【書類名】 要約書**【要約】**

【課題】 アクセス制御ポリシーの設定を、各ソフトウェアの仕様を知らなくても適切に設定、且つ維持可能なポリシー設定支援ツールを提供する。

【解決手段】 ソフトウェアの種類毎のポリシーを記述したサンプル情報と、オブジェクトの種類毎に利用頻度の高いプログラムの情報を記述した関連付け情報と、プログラムの動作を監視して記録したアクセスログ情報のいずれかを用いてポリシーの原案を作成するポリシー生成部 1 0 2 と、ポリシー原案を表示して、利用者による確認と編集を可能とするユーザインタフェース部 1 0 1 の処理により、適切なポリシー設定に必要な作業の簡易化を実現する。また差分検出部 1 0 4 により、設定済みポリシーから更新すべき部分を、現在のオブジェクト 1 1 2 とサブジェクト情報 1 1 3 を参照して検出し、ユーザインタフェース部 1 0 1 を通じて提示するとともに、簡易に更新可能とすることで、適切なポリシー維持も可能とする。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 0 2 4 3 9
受付番号	5 0 2 0 1 5 5 9 7 1 1
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 4 年 1 0 月 1 8 日

＜認定情報・付加情報＞

【提出日】 平成14年10月17日

次頁無

特願 2 0 0 2 - 3 0 2 4 3 9

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所